CATEGORIAS

* Constrained device - Class 0
* Constrained device - Class 1
* Constrained device - Class 2
* High-capacity device

DISPOSITIVOS

|  |  |  |
| --- | --- | --- |
| Nombre | Categoría | Icono |
| iPhone 12 | High-capacity device | https://i.imgur.com/O0cnwUV.jpg |
| TP-LINK Archer C50 | High-capacity device | https://i.imgur.com/2Txmbm9.jpg |
| Amazon echo dot | High-capacity device | https://i.imgur.com/wSJQS6n.jpg |
| HP OfficeJet Pro | High-capacity device | https://i.imgur.com/703D8Kf.jpg |
| Lenovo ThinkPad T440s | High-capacity device | https://i.imgur.com/q3hit4x.jpg |
| Playstation 3 | High-capacity device | https://i.imgur.com/fWhU1zr.jpg |
| Samsung Smart TV X10P | High-capacity device | https://i.imgur.com/S15N7Ke.jpg |
| Pebble Smartwatch | High-capacity device | https://i.imgur.com/RJBXOi9.jpg |
| Radio Thermostat CT80 | Constrained device - Class 2 | https://i.imgur.com/g5RMyjd.png |
| TPLink Tapo L530 | Constrained device - Class 1 | https://i.imgur.com/QbGQQRs.jpg |
| Samsung Galaxy S5 | High-capacity device | https://i.imgur.com/YExRit4.jpg |
| iPhone 13 | High-capacity device | https://i.imgur.com/O3UGkJZ.jpg |

CONTROLES (Uso solo los de Usage until end-of-life)

Interfaz de usuario gráfica

Descripción generada automáticamente

|  |  |  |  |
| --- | --- | --- | --- |
| Id | Nombre | Descripción | Categoría |
| 1 | Protección de intercambio de datos: Asegurar los derechos de acceso | Los usuarios deben verificar las autorizaciones otorgadas a los dispositivos y servicios para acceder e intercambiar datos. Esto es especialmente importante en caso de una actualización, donde los derechos de acceso pueden modificarse sin el consentimiento del usuario. Por ejemplo, los dispositivos y servicios pueden mostrar una vista completa de sus comunicaciones con dispositivos y servicios externos, su necesidad de utilizar datos privados, etc. | 0+ |
| 2 | Protección de intercambio de datos: Utilizar gateways para reducir la exposición de red de los dispositivos más débiles | Las redes locales deben estar separadas siempre que sea posible. Cada una de estas redes debe estar protegida por un gateway dedicado (ya sea porque consisten en dos redes diferentes o porque consisten en dos VLAN diferentes gestionadas por un gateway). | 0+ |
| 3 | Protección de intercambio de datos: Segregar las Redes del Hogar Inteligente y el AMI (infraestructura de medición avanzada) | Cumplir con los requisitos y recomendaciones del gateway AMI si se instala un Medidor Inteligente. En algunas arquitecturas la pasarela hacia la Infraestructura de Medición Avanzada se utiliza como una interfaz hacia la Red de Área del Hogar. Para asegurar el correcto funcionamiento de la AMI, los proveedores de Hogar Inteligente deberían:  - implementar la protección requerida por la pasarela inteligente, si es necesaria; y  - evitar la interrupción del servicio, por ejemplo, causando una denegación de servicio al utilizar demasiado ancho de banda. | 0+ |
| 4 | Seguridad operativa y mantenimiento - Evaluación de vulnerabilidades: Realizar evaluaciones de vulnerabilidad | Una vez que un dispositivo está en el mercado, el proveedor debe llevar a cabo una evaluación de vulnerabilidades y corregir las fallas de seguridad en consecuencia. La evaluación de vulnerabilidades debe incluir hallazgos del desarrollador, investigaciones en línea, avisos de CERTs, así como aportes de clientes e investigadores de seguridad. Se debe informar al usuario final sobre el período de soporte del dispositivo y sobre el fin del soporte para correcciones de seguridad.  Se debe definir una política para el manejo de vulnerabilidades y concientización sobre divulgación. Los programas de recompensa por errores también pueden proporcionar un incentivo para los investigadores externos.  Las vulnerabilidades conocidas deben ser corregidas. Un parche puede consistir en una solución temporal si el desarrollador aún no ha proporcionado una solución definitiva. Cuando las actualizaciones por aire no estén disponibles, se debe considerar un plan para retirar el producto, de modo que los proveedores puedan implementar el parche en los dispositivos.  Para los servicios en línea que respaldan los dispositivos del Hogar Inteligente, debe ser posible revertir a un estado seguro.  En última instancia, las vulnerabilidades que afecten los datos de usuario deben comunicarse de la manera más transparente posible. La Opinión 03/2014 de la Unión Europea sobre la Notificación de Brechas de Datos Personales del Grupo de Trabajo del Artículo 29 proporciona ejemplos de tales situaciones. | 0+ |
| 5 | Seguridad operativa y mantenimiento - Evaluación de vulnerabilidades: Verificar regularmente las suposiciones de seguridad durante el tiempo de vida | Los dispositivos y servicios realizaron suposiciones para asegurarse de que los requisitos de seguridad son suficientes. Se alienta a los proveedores y usuarios a verificar regularmente que estas suposiciones sigan siendo válidas. Por ejemplo:  - Limitaciones en el uso del dispositivo (por ejemplo, un dispositivo determinado podría necesitar conectividad ZigBee para transmitir alarmas de seguridad, lo que implica que no podrá enviar alarmas cuando esté ubicado detrás de una pared muy gruesa). Los proveedores podrían descubrir que, en el campo, la señal requiere incluso condiciones más estrictas (paredes aún más delgadas, sin interferencias...). Necesitarán enviar a los usuarios información para que puedan verificar si su instalación es segura.  - Propiedades asumidas del entorno (por ejemplo, suponer que todas las autoridades de certificación en el almacén de certificados son confiables y no están comprometidas). Los proveedores deben realizar una evaluación para poder eliminar una CA comprometida del almacén de certificados.  - Propiedades asumidas de propiedades criptográficas (por ejemplo, asumir que un determinado algoritmo y tamaño de clave son suficientes para una tarea determinada). Los proveedores deberán verificar regularmente esta suposición, por ejemplo, si un nuevo ataque criptográfico pone en riesgo a los usuarios a menos que utilicen claves más largas o cambien sus conjuntos criptográficos. | 0+ |
| 6 | Seguridad operativa y mantenimiento - Actualizaciones de seguridad: Proteger el mecanismo de actualización de software | Las actualizaciones de seguridad ofrecen protección contra vulnerabilidades encontradas durante la vida útil de un dispositivo o aplicación. Sin embargo, esto tiene un costo, ya que el soporte de esta funcionalidad también proporciona un punto de entrada para un atacante. En particular, los proveedores deben:  - Proporcionar actualizaciones de seguridad automáticas y oportunas.  - Proteger las actualizaciones (típicamente a través de encriptación y firma digital). Los archivos de actualización no deben contener datos sensibles. La firma debe ser verificada antes de que se aplique la actualización. Proteger la aplicación de una actualización en el dispositivo. Un atacante no debería poder iniciar una instalación de firmware sin autorización.  - Proteger la interfaz de actualización de seguridad contra ataques. | 1+ |
| 7 | Seguridad operativa y mantenimiento - Protección de interfaces remotas: Proporcionar interfaces amigables para la gestión de seguridad de dispositivos y servicios | La facilidad de uso de la interfaz de usuario debe contribuir a ayudar a los usuarios a realizar tareas administrativas correctas. Tales interfaces pueden encontrarse, por ejemplo, en el propio dispositivo, en un portal web o a través de una aplicación móvil. La amigabilidad con el usuario ayuda a mantener un estado seguro en el dispositivo al:  - Dar más posibilidades de que acciones simples como una actualización de firmware o cambios de contraseña sean realizadas efectivamente por el usuario.  - Proporcionar una descripción precisa del estado de seguridad del servicio y explicar qué acciones pueden contribuir a mitigar posibles amenazas.  Los proveedores y prestadores de servicios también deberían sensibilizar a sus usuarios sobre correos electrónicos infectados y bulos. | 1+ |
| 8 | Seguridad operativa y mantenimiento - Protección de interfaces remotas: Proteger las interfaces de monitoreo remoto | La protección de las interfaces de monitoreo remoto es crucial, ya que a menudo proporcionan un punto de entrada altamente privilegiado en un dispositivo. Esta protección incluye mecanismos de control de acceso y autenticación. | 1+ |
| 9 | Seguridad operativa y mantenimiento - Sistema de gestión de seguridad para infraestructuras de soporte: Confiar en fuentes existentes de buenas prácticas de seguridad para asegurar las infraestructuras | En cuanto a los requisitos para infraestructuras remotas relacionadas con el Hogar Inteligente, no hay necesidades específicas en el caso de uso del Hogar Inteligente en comparación con los servicios en la nube habituales o las infraestructuras de soporte de dispositivos habituales.  Por esta razón, las principales recomendaciones consistirían en:  - Gestión de seguridad: Como regla general, implementar un sistema de gestión de seguridad de la información (SGSI) como se describe en la norma ISO 27001. Se aplican las recomendaciones de ENISA.  - Desarrollo seguro: como regla general, seguir las recomendaciones emitidas por OWASP.  - Evaluación de seguridad: recomendamos que los operadores de servicios:  > Soliciten auditorías de terceros en sus infraestructuras (estas auditorías pueden ser parte de una certificación ISO 27001).  > Soliciten pruebas de penetración de terceros de sus servicios, incluyendo al menos un escaneo de red y, si es posible, pruebas de penetración manuales.  En cuanto a la computación en la nube, los proveedores de servicios deben considerar la certificación siguiendo las recomendaciones de ENISA. | 1+ |
| 10 | Control de datos de usuario: Proporcionar copias de seguridad seguras y/o eliminación de los datos almacenados/procesados por el dispositivo (y por los servicios en la nube asociados) durante la operación y al final de su vida útil | El usuario final debe contar con un medio para borrar de manera segura sus datos privados recopilados o almacenados en un dispositivo del Hogar Inteligente.  De manera más general, debería estar disponible en el dispositivo una opción para realizar un restablecimiento seguro de fábrica del firmware y la configuración.  Para la información del cliente en infraestructuras remotas como servicios en la nube, se debe contar con un proceso de sanitización de datos.  En cuanto a los datos del usuario presentes en los dispositivos, la eliminación segura de las claves de encriptación puede proporcionar suficiente protección, siempre y cuando los datos estén encriptados en condiciones que garanticen la confidencialidad a largo plazo.  Los metadatos deben ser borrados de la misma manera que otros datos sensibles, ya que aplican las mismas amenazas. | 1+ |

AMENAZAS

|  |  |  |  |
| --- | --- | --- | --- |
| Id | Nombre | Controles para mitigarlo | Descripción |
| 1 | Fraude de identidad | 4,5,6,7,8,9 | El fraude de identidad debe ser abordado no solo mediante la protección de credenciales, sino también mediante la protección de datos privados que podrían contribuir a la suplantación de identidad. Por lo tanto, esto también está cubierto por medidas de privacidad. |
| 2 | Correo electrónico no solicitado e infectado/Broma | 4,5,6,7,8,9 | Este tema típicamente puede ser abordado a través de campañas de concientización por parte de los proveedores y prestadores de servicios. |
| 3 | Denegación de servicio | 4,5,6,7,8,9 | Mecanismos de seguridad, multiplicidad de interfaces y notificaciones al usuario deben asegurar un nivel mínimo de robustez contra la denegación de servicio. La protección de las comunicaciones también aborda estas preocupaciones. |
| 4 | Actividad de software/código malicioso | 4,5,6,7,8,9 | La autodefensa debe abarcar las vulnerabilidades relacionadas con código malicioso. Otra forma de mitigar estas amenazas consiste en proporcionar protección adicional en la Red de Área del Hogar y gestionar relaciones de confianza para aislar dispositivos comprometidos. |
| 5 | Abuso de fuga de información | 1,2,3,4,5,6,7,8,9,10 | Las funciones de administración de seguridad también deben estar disponibles (gestión de seguridad). En última instancia, el diseño debe llevar a interfaces de usuario comprensibles y utilizables. Los requisitos de privacidad y confidencialidad también requieren transparencia, para que el usuario esté consciente del tipo de datos que podrían estar potencialmente en riesgo. |
| 6 | Manipulación de información | 4,5,6,7,8,9 | Las relaciones de confianza y reputación, asociadas a la protección de la comunicación, deben cubrir los riesgos de manipulaciones de información externa. No debe ser posible manipular el registro de auditoría. |
| 7 | Acceso no autorizado al sistema/red de información - Uso no autorizado de la administración de dispositivos y sistemas - Abuso de autorizaciones | 4,5,6,7,8,9 | La identificación, autenticación y autorización son requisitos generales para el acceso a funciones sensibles. Esto es especialmente importante en el caso de capacidades administrativas. |
| 8 | Instalación no autorizada de software - Software malicioso | 4,5,6,7,8,9 | La gestión de seguridad también establece que la instalación de firmware debe estar protegida para asegurar su autenticidad e integridad. |
| 9 | Actividad remota (ejecución) | 4,5,6,7,8,9 | Las capacidades remotas de un dispositivo deben estar disponibles solo para usuarios autorizados y deben llevarse a cabo a través de canales seguros. |
| 10 | War driving | 4,5,6,7,8,9 | Los dispositivos y servicios deben implementar comunicaciones seguras. Sin embargo, hay algunos dispositivos que carecen de capacidades para esto y, en el caso de "war driving", el atacante apunta a la Red de Área del Hogar. Por esta razón, la protección de red adicional en la Red de Área del Hogar es particularmente crítica con respecto a esta amenaza. |
| 11 | Falta de recursos/electricidad - Corte de Internet - Corte de red – Huelga - Pérdida de servicios de soporte | 4,5,6,7,8,9 | Los mecanismos de seguridad, la diversidad de interfaces y las notificaciones al usuario deben asegurar que los cortes de energía o de red no obstaculicen la seguridad. |
| 12 | Fuga o intercambio de información - Uso o administración errónea de dispositivos y sistemas | 4,5,6,7,8,9 | Las funciones de administración de seguridad también deben estar disponibles (gestión de seguridad). Eventualmente, el diseño debería conducir a interfaces de usuario comprensibles y utilizables. Los requisitos de privacidad y confidencialidad también requieren transparencia, para que el usuario esté consciente del tipo de datos que podrían estar potencialmente en riesgo. |
| 13 | Fuga de información | 4,5,6,7,8,9 | La protección de los datos del usuario incluye medidas para asegurar que estos datos no se filtren accidentalmente. La orientación al usuario contribuye a educar al usuario final en este sentido. |
| 14 | Fallas o interrupciones de enlaces de comunicación (redes de comunicación) - Fallas o interrupciones del suministro principal - Fallas o interrupciones del suministro eléctrico | 4,5,6,7,8,9 | Los mecanismos de seguridad a prueba de fallos, la diversidad de interfaces y las notificaciones al usuario deben asegurar que los cortes de energía o de red no obstaculicen la seguridad. |
| 15 | Errores de configuración | 4,5,6,7,8,9 | El diseño debe llevar a interfaces de usuario comprensibles y utilizables. La orientación al usuario también contribuye a ayudar al usuario a tomar decisiones de configuración sensatas. |